



TITLE:

On a normal integral basis problem over cyclotomic \mathbb{Z}_p -extensions (Algebraic Number Theory and Related Topics)

AUTHOR(S):

市村, 文男

CITATION:

市村, 文男. On a normal integral basis problem over cyclotomic \mathbb{Z}_p -extensions (Algebraic Number Theory and Related Topics). 数理解析研究所講究録 2003, 1324: 67-75

ISSUE DATE:

2003-05

URL:

<http://hdl.handle.net/2433/43147>

RIGHT:

On a normal integral basis problem over cyclotomic \mathbb{Z}_p -extensions

横浜市立大学数理学教室 市村 文男 (Humio Ichimura)
Department of Mathematical Science,
Yokohama City University

§1 序文

講演ではまず Hilbert-Speiser の定理に関連するいくつかの話題を述べた後、特殊な設定の下ではあるが、ある種の素数次巡回拡大が normal integral basis を持つか否かを p 進関数が生々しく支配している事を報告した。内容は私の論文 [1], [2], [3] にもとずいている。以下、記号を導入した上で、問題と得られた結果を述べる。

§2 設定と問題

代数体の有限次ガロア拡大 L/K が normal integral basis (NIB) を持つとは、 \mathcal{O}_L が群環 $\mathcal{O}_K[\text{Gal}(L/K)]$ と cyclic になる事を言う。ここで、 \mathcal{O}_K は K の整数環である。Noether により、 L/K が NIB を持てば、 L/K は tame である。NIB にまつ

古典的な問題のひとつは、 $kame$ なガロア拡大全体のなかで NIB を持つものがどのくらいあるかという問である。

以下、 p を奇素数、 K を ζ_p を含む虚アーベル体、 k_∞/K を円分群拡大、 K_m をその m 番目の中間体とする。但し、 $k_0 = K$ 。

$$\Sigma_m := \{a \in \mathcal{O}_{K_m} \mid a \mathcal{O}_{K_m} : \text{square free}, a \equiv 1 \pmod{p}, \forall p \mid p\}$$

とし、 $a, b \in \Sigma_m$ に対して $a \sim b$ を $K_m(a^{1/p}) = K_m(b^{1/p})$ となる事と定める。集合 $\mathcal{S}_m, \mathcal{I}_m, \mathcal{N}_m$ を次の様に定義する。

$$\mathcal{S}_m := \Sigma_m / \sim,$$

$$\mathcal{I}_m := \{[a]_m \in \mathcal{S}_m \mid K_m(a^{1/p})/K_m : kame\},$$

$$\mathcal{N}_m := \{ \quad \quad \mid \quad \quad : \text{NIB を持つ} \}.$$

Noether により、 $\mathcal{N}_m \subseteq \mathcal{I}_m$ である。 $m > n$ の時、自然な写像 $K_n \rightarrow K_m$ は単射 $\mathcal{I}_n \rightarrow \mathcal{I}_m$ を誘導するので、以下 $\mathcal{I}_n \subseteq \mathcal{I}_m$ とみなす。この時、 $\mathcal{N}_n \subseteq \mathcal{N}_m$ である。集合 $\mathcal{I}_m \cap \mathcal{N}_m$ は、 $[a]_m \in \mathcal{I}_m$ で $K_m(a^{1/p})/K_m$ が NIB を持つものの全体である。

講義で扱った問題は次の二つである：

問 1 (古典的問題) \mathcal{I}_m 内で \mathcal{N}_m はどのくらい大きいか小さいか？

問 2 (単項化の問題) $m > n$ の時、 $\mathcal{I}_m \cap \mathcal{N}_m$ は \mathcal{I}_m 内でどのくらい大きいか小さいか？

問 2 は、イデアル類群についての次の良く知られた事実を意識して設定した。 A_m を K_m のイデアル類群の p -part,

$A_\infty = \varinjlim A_m$ をその順極限とする。これらの群は複素共役の作用で分解される。

事実 (i) $m > n$ の時、自然な写像 $A_m \rightarrow A_n$ は単射、

(ii) A_∞ の構造は p 進 L 関数で記述される (Mazur-Wiles の定理),

(iii) $A_\infty^\tau = 0$ (Greenberg 予想)。

この事実の類似が成り立つというのが問 2 の内容である。

§3 結果 1

イデアル類群の場合と同じ様に \mathcal{J}_m も複素共役の作用で分解したい。 \mathcal{U}_m を K_m の p での主 semi-local units の群とする。更によく知られている様に、 $[a]_m \in \mathcal{S}_m$ に対して、

$$[a]_m \in \mathcal{J}_m \iff a \equiv u^p \pmod{\pi^p}, \exists u \in \mathcal{U}_m.$$

但し、 $\pi = \zeta_p - 1$ 。そこで、

$$\mathcal{J}_m^\pm := \{ [a]_m \in \mathcal{J}_m \mid a \equiv u^p \pmod{\pi^p}, \exists u \in \mathcal{U}_m^\pm \}$$

と定める。 u として 1 をとれば、 $\mathcal{J}_m^+ \cap \mathcal{J}_m^-$ が無限集合である事がわかる。しかし、実は $\mathcal{J}_m^+ \cap \mathcal{J}_m^- \subseteq \mathcal{N}_m$ なので問題は無い。

命題 1 $p \nmid [K:\mathbb{Q}]$ の時、次が成り立つ:

(i) $\mathcal{J}_0 = \mathcal{N}_0$,

(ii) $\mathcal{J}_m^+ \cap \mathcal{N}_m$ は \mathcal{J}_m^- 内で“非常に小さい”, $\forall m \geq 1$,

$$(iii) \quad J_m \cap N_m \subseteq N_m, \quad \forall m > n \geq 0.$$

(iii) は、 $A_m \rightarrow A_m$ の単射性の類似である。以下、 J_m^+ を扱う。
次の仮定の下で話を進める。

(c1) $\Delta = \text{Gal}(K/\mathbb{Q})$ の exponent は $p-1$ 。

(c2) p 上の K の素点は唯一つ。

命題 2 (c1), (c2) の下で、 $p \nmid h_K^- = h_K/h_{K^+} \Rightarrow J_m^+ \subseteq N_m, \forall m \geq 1$ 。
但し、 h_K は K の類数である。

この命題は、Kummer duality $p \nmid h_K^- \Rightarrow p \nmid h_{K^+}$ と良く似ている。
以下、 $p \mid h_K^-$ の場合を扱う。そのため、 J_m を Δ の作用により細かく分解する。 $\chi \in \hat{\Delta}$ を \mathbb{Q}_p -値の偶指標、 $\chi^* = \omega \chi^{-1}$ をその双対とする。但し、 ω は Δ の \mathbb{F}_p の作用を表わす指標である。

$$J_m(\chi) := \{ [a]_m \in J_m \mid a \equiv u^p \pmod{\pi^p}, \exists u \in \mathcal{U}_m(\chi) \}$$

と定める。 Δ の自明な指標 χ_0 に対して、 $A_m(\chi_0) = 0$ が知られている (Stickelberger の定理)。この類似として次が成り立つ。

命題 3 $J_m(\chi_0) \subseteq N_m, \forall m \geq 1$ 。

以下、 $\chi \in \hat{\Delta}$ を非自明な偶指標とする。(c1), (c2) に加えて

次を仮定する。

$$(C3) \quad A_0(X^*) \neq 0.$$

$g_X(T) \in \Lambda = \mathbb{Z}_p[[T]]$ を p 進 L 関数 $L_p(s, X)$ に対応する巾級数とする；
 $g_X((1+p)^{1-s}-1) = L_p(s, X).$

$P_X(T)$ を g_X に付随する distinguished な多項式とする。 $\lambda_X^* = \deg P_X$ とおく。(C3) より $\lambda_X^* \geq 1$ である。 I_m を $p^m, p^{m-1-j}T^{p^j} (0 \leq j \leq m-1)$ で生成された Λ のイデアルとする。この時、次が成り立つ。

定理 1 仮定 (C1) ~ (C3) の下で更に $A_0(X) = 0$ と仮定する。

$$(1) \quad |J_m(X) \setminus N_m| = \infty, \quad \forall m \geq 1.$$

$$(2) \quad p^{m-1}(p-1) \geq \lambda_X^* \text{ の時: } J_m(X) \cap N_m \subseteq N_m, \quad \forall m \geq m.$$

$$(3) \quad p^{m-1}(p-1) \leq \lambda_X^* \leq p^m \text{ の時:}$$

$$(i) \quad |J_m(X) \setminus N_{m+1}| = \infty,$$

$$(ii) \quad T^{p^m - \lambda_X^*} P_X \notin I_m \Rightarrow |(J_m(X) \cap N_{m+1}) \setminus N_m| = \infty,$$

$$" \in I_m \Rightarrow J_m(X) \cap N_{m+1} \subseteq N_m.$$

$$(4) \quad p^m \leq \lambda_X^* \text{ の時:}$$

$$(i) \quad p \nmid P_X(0) \Rightarrow J_m(X) \subseteq N_{m+1}.$$

$$p^2 \mid P_X(0) \Rightarrow |J_m(X) \setminus N_{m+1}| = \infty,$$

$$(ii) \quad P_X \notin I_{m+1} \Rightarrow |(J_m(X) \cap N_{m+1}) \setminus N_m| = \infty$$

$$P_X \in I_{m+1} \Rightarrow J_m(X) \cap N_{m+1} \subseteq N_m.$$

$$(5) \quad m > n \geq 1 \text{ に對して,}$$

$$J_m(X) \not\subseteq N_{m-1} \text{ だが } J_m(X) \subseteq N_m$$

$$\Leftrightarrow \text{(i) } \lambda_X^1 \geq p^m, \text{ (ii) } p^{m-m} \parallel P_X(0), \text{ (iii) } P_X \in (p^{m-m}, I_m).$$

(2)により、大きい m に対しては、“単項化”の現象は起らない。つまり、Greenberg 予想の類似は整数環では成り立たない。(3)~(5)では、小さい m に対しては“単項化”の現象が起り得て、実際に起こるかどうかを p 進 L 関数 $P_X(T)$ が支配している事をいっている。

例 (陽田浩樹氏による) $p=3, K=\mathbb{Q}(\sqrt{-3}, \sqrt{d}), d>0$ とする。
 χ を Δ の唯一の非自明偶指標とする。

$d=269681$ で $(m, m)=(1, 2), (2, 3)$ で (5) の (i), (ii), (iii) の条件がみたされている,

$d=9340977$ で $(m, m)=(1, 3)$ で (5) の (i), (ii), (iii) の条件が成立。

§4 結果2 (主結果)

E_m, C_m をそれぞれ K_m の単数群, 円単数群とし, $E_m = \overline{E_m \cap U_m}$, $C_m = \overline{C_m \cap U_m}$ とする。 $U_m^{(1)} = \{u \in U_m \mid u \equiv 1 \pmod{\pi}\}$ とする。
 §3 で述べた様に, $[a]_m \in S_m$ に対して, $[a]_m \in J_m \Leftrightarrow a \equiv u^p \pmod{\pi^p}, \exists u \in U_m$ である。この $u = u_a$ は $U_m^{(1)}$ を法として一意に定まる。次の主張が、問1, 問2と岩澤理論もつなぐ橋である。

る。

key Lemma $[a]_m \in \mathcal{J}_m$ に対して、

$$[a]_m \in \mathcal{N}_m \iff a \equiv \varepsilon^p \pmod{\pi^p}, \exists \varepsilon \in \mathcal{E}_m$$

$$(\iff u_a \in \mathcal{E}_m \mathcal{U}_m^{(1)}).$$

この補題により、 $m \geq n$ に対して、

$$(*) \quad [a]_m \in \mathcal{N}_m \iff u_a \in \mathcal{E}_m \mathcal{U}_m^{(1)}$$

である。そこで写像 θ_m を

$$\theta_m: \mathcal{J}_m^+ \longrightarrow (\mathcal{U}_m / \mathcal{E}_m \mathcal{U}_m^{(1)})^+, [a]_m \mapsto \bar{u}_a$$

で定める。 θ_m は全射である事、各類 $\bar{u} \in (\mathcal{U}_m / \mathcal{E}_m \mathcal{U}_m^{(1)})^+$ に対して $\theta_m^{-1}(\bar{u})$ が無限集合になる事が容易にわかる。 $(*)$ にからがみ

$$H_{m,m} = \ker(\mathcal{U}_m \longrightarrow \mathcal{U}_m / \mathcal{E}_m \mathcal{U}_m^{(1)}, u \mapsto u \bmod \mathcal{E}_m \mathcal{U}_m^{(1)})^+$$

と置く。容易に、 $H_{m,m} \subseteq H_{m,m+1}$ 、 $(*)$ より、

$$\mathcal{J}_m^+ \cap \mathcal{N}_m = \theta_m^{-1}(\bar{1})$$

$$\mathcal{J}_m^+ \cap \mathcal{N}_m = \theta_m^{-1}(\bar{H}_{m,m}) \quad (\text{但し、}\bar{H}_{m,m} = H_{m,m} \bmod \mathcal{E}_m \mathcal{U}_m^{(1)})$$

となる。従って、問1, 問2は、filtration

$$(\mathcal{U}_m^{(1)} \mathcal{E}_m)(X) = H_{m,m}(X) \subseteq H_{m,m+1}(X) \subseteq \cdots \subseteq H_{m,m}(X) \subseteq \cdots \subseteq \mathcal{U}_m(X)$$

を調べよという問題に帰着する。 \mathcal{U}_m について次の事が知られて

いる。 $w_m = (1+T)^{p^m} - 1$, $v_{m,m} = w_m / w_m$ ($m \geq n$) と置く。

$$(1) \quad \mathcal{U}_m(X) \simeq \Lambda / (w_m),$$

$$(2) \quad U_m^{(1)}(X) \simeq I_m / (w_m),$$

$$(3) \quad A_0(X) = 0 \Rightarrow E_m(X) = E_m(X) \simeq (P_X, w_m) / (w_m).$$

従って、

$$G_{m,m} = (P_X, I_m),$$

$$G_{m,m} = \ker(\Lambda \rightarrow \Lambda / G_{m,m}; \alpha \mapsto \overline{V_{m,m}\alpha}), \quad m \geq n$$

とよくと、 $H_{m,m}(X) \simeq G_{m,m} / (w_m)$, $\forall m \geq n$, と取り、結局、我々の問題は、 Λ の FIPV の filtration

$$G_{m,m} \subseteq G_{m,m+1} \subseteq \cdots \subseteq G_{m,m} \subseteq \cdots \subseteq \Lambda$$

を調べる事に帰着する。

定理 2 以上の設定の下で次が成り立つ。

(1) 商 $G_{m,m+1} / G_{m,m}$ は Λ 加群として cyclic であり、その Λ 上の生成元は $P_X(T)$ から出発して $m-n$ に関して“帰納的”に計算できる。

(2) $m = n$ とする。

$$h_X = (P_X - T^{\lambda_X^*}) / p,$$

$$p^m \leq \lambda_X^* \Rightarrow A = h_X, \quad p^m \geq \lambda_X^* \Rightarrow A = T^{p^m - \lambda_X^*} h_X \quad \text{とよくと、}$$

$G_{m,m+1} / G_{m,m}$ は Λ 上 A の類で生成される。

定理 1 の大部分は定理 2 をもとにした多少の計算によって得られる。

参考文献

- [1] H. Ichimura, Note on the ring of integers of a kummer extension of prime degree, III, Proc. Japan Acad., 77A (2001), 71-73.
- [2] H. Ichimura, On a normal integral basis problem over cyclotomic \mathbb{Z}_p -extensions, II, J. Number Theory, 96 (2002), 105-132.
- [3] H. Ichimura, On some ideals of the p -adic power series ring arising from a normal integral basis problem, 投稿中.